Examples of Requirements Problems Found Via Formal Inspections

by
Hernan Guarda
Software Product Assurance Section
Jet Propulsion laboratory, California institute of Technology

On many]1'1, projects, one of the critical subsystems or elements in the design of the Ground System is the Uplink Operations Element. On one project, the Uplink Operations Element team decided to carry out inspections on their design documents in order to increase the level of assurance and quality of their products. The first document to undergo inspection was the Uplink Operations Element Functional Requirements 1)ocument. The scope of this document is so large that the text is really a description of the work to be performed by the Element. Children documents address more detailed interface needs such as file formats and data structures. The following describes two issues which arose during inspections of these requirements, and shows how the requirements changed to address the' issues.

Issue 1

Requirement Prior to Formal Inspection:

> The Ground System shall be capable of generating commands to restart a sequence which has been halted by fault protection response.

Explanation:

> This requirement on the Uplink Operations Element implies that the engineers can restart a command sequence to the spacecraft knowing that fault conditions have been detected and the Command ant] Data Subsystem (Cl)S) software has determined that it is unable to proceed in its computations and has invoked fault processing.

issue(s) Raised:

> The Ground System needs to know the rationale behind the requirement in order to satisfy unclear specifications. The kind of additional in formation that needs to be specified are, for example, under what conditions would a restart be used in preference to a C1)S stored sequence reload? in addition, the Ground System needs to know under what conditions would a reload not work, and most importantly, when would a reload pose a significant threat to the mission?

"1 he Rewri t ten Requirement:

> The Uplink Operations Element shall be able to restart a sequence to cause restart of a previously loaded sequence in cases where more than 1 week of execution time remains in the previously loaded sequence.

Issue 2

Requirement 1 'rim to Formal Inspection:

The Ground System shall execute a recovery response within a period of two weeks following an anomaly,

Explanation:

This requirement scopes the time needed for recovery from an anomaly, Under certain situations this parameter is crucial because certain sequences cannot be designee], tested under simulation, and verified under short notice. in some situations, recovery scenarios must be constructed in advance or the mission operations team must have a skeleton that is tailored to the specific circumstances.

Issue(s) Raised:

Critical sequences and trajectory correction maneuvers for earth swing-by will have much shorter response times.

'1 he Rewritten Requirement:

The Uplink Operations Element shall generate a recovery response sequence within a period of three days.

1 discussion

in general, the Formal Inspection l'recess helped enormously in the revision of the Uplink Operations Element Functional Requirements Document because it identified areas that lacked sufficient definition for the work to proceed to the next level of refinement.

Acknowledgements

The work described in this paper was carried out by the Jet l'repulsion '1 aboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.